Single Port KVM over IP

User Manual

V1.1

2007.7.6

Certifications

FCC

This equipment has been tested and found to comply with Part 15 of the FCC Rules.
Operation is subject to the following two conditions:

(1) This device may not cause harmful interference
(2) This device must accept any interference received, including interference that may cause undesired operation.

CE

This equipment is in compliance with the requirements of the following regulations:
EN 55022: CLASS B

RoHS

All contents of this package, including products, packing materials and documentation comply with RoHS.

Contents

1. Product Overview 5
1.1 Introduction 5
1.2 Main Feature 5
2. Installation and Start up 6
2.1 Package Check List 6
2.2 Panel Views 6
2.3 Rack Mounting 7
2.4 Cable Connections 8
2.5 LED Indicators, Button 9
2.6 Startup Guide 9
2.6.1 A Network Setup Software Tool -- IP Setup 9
3. Managements Overview 11
3.1 Access Privileges and Session Timeout 11
3.2 Web Browser Management Interface 13
4. General Information 14
5. Configuration 15
5.1 Network 15
5.2 DNS and Dynamic DNS 16
5.3 NTP (Date and time) 17
5.4 SMTP 18
5.5 Mouse Mode 19
5.6 Image Quality 19
5.7 Serial over LAN 19
5.8 Users 20
5.9 SSL Certificate 20
5.10 LDAP 21
6. Remote Control 22
6.1 Remote KVM Console 22
6.2 Special Settings for ActiveX 27
7. Serial Power Control 30
8. Maintenance 31
8.1 Firmware Upgrade 31
8.1.1 Upgrade from web page 31
9. System Log 35
10. Technical Data 36
10.1 Technical Specifications 36
10.2 Default Settings 37

Appendix A: Ethernet pin-outs (RJ-45) 38
Appendix B: Well-Known TCP/UDP Port Numbers 39
Appendix C: Protocol Glossary 40

F i g u r e s

Figure 1 Panel Views 6
Figure 2 Rack Mount Installation 7
Figure 3 Cable Connections 8
Figure 4 Dynamic DNS 17
Figure 5 Serial Power Control 30

1. Product Overview

1.1 Introduction

The IP-KVM switch redirects local keyboard, mouse and video data to a remote administration console. It allows you to control one or many computers locally at the server site or remotely via the Internet using a standard browser. You can securely gain BIOS level access to systems for maintenance, support, or failure recovery over the Internet. Communication is secure via SSL authentication and encryption. Use in conjunction with a KVM switch for multiple-server access.

The IP-KVM provides convenient, remote KVM access and control via LAN or Internet. It captures, digitizes, and compresses video signal and transmits it with keyboard and mouse signals to and from a remote computer. IP-KVM provides a non-intrusive solution for remote access and control. Remote access and control software runs on its embedded processors only but not on mission-critical servers, so that there is no interference with server operation or impact on network performance.

1.2 Main Feature

- Manage servers around the world.
- Zero-U rack mountable
- KVM (keyboard, video, and mouse) access over IP or analogous telephone line (modem needed).
- Full control under any OS, in BIOS mode, during boot, at Blue Screens
- No additional software necessary on servers
- SSL Certificate management
- 256-bit SSL encryption of all transmitted data
- Automatically senses video resolution for best possible screen capture
- High-performance mouse tracking and synchronization
- Automatic adjustment of data rate to transmission line
- Remote mass storage control and redirection
- Can be remote controlled over ActiveX or java-enabled Browsers
- Firmware update via web interface
- Port to connect a user console for direct analogous access to KVM switch
- Can be used with most standard KVM

2. Installation and Start up

2.1 Package Check List

The IP-KVM package consists of followings items:

1x the single port IP-KVM unit
1x CD-ROM (software utilities and User's manual)
1x Quick Start Guide
1x AC to DC Power Adapter (DC 5V / 2.5A)
1x Power Cord cable (6 feet)
1x Rack Mount Kit (Brackets and screws)
1x Null modem cable (6 feet)
1x USB A-to-B cable (6 feet)
1x 3-to-3 KVM cable (3 feet)

2.2 Panel Views

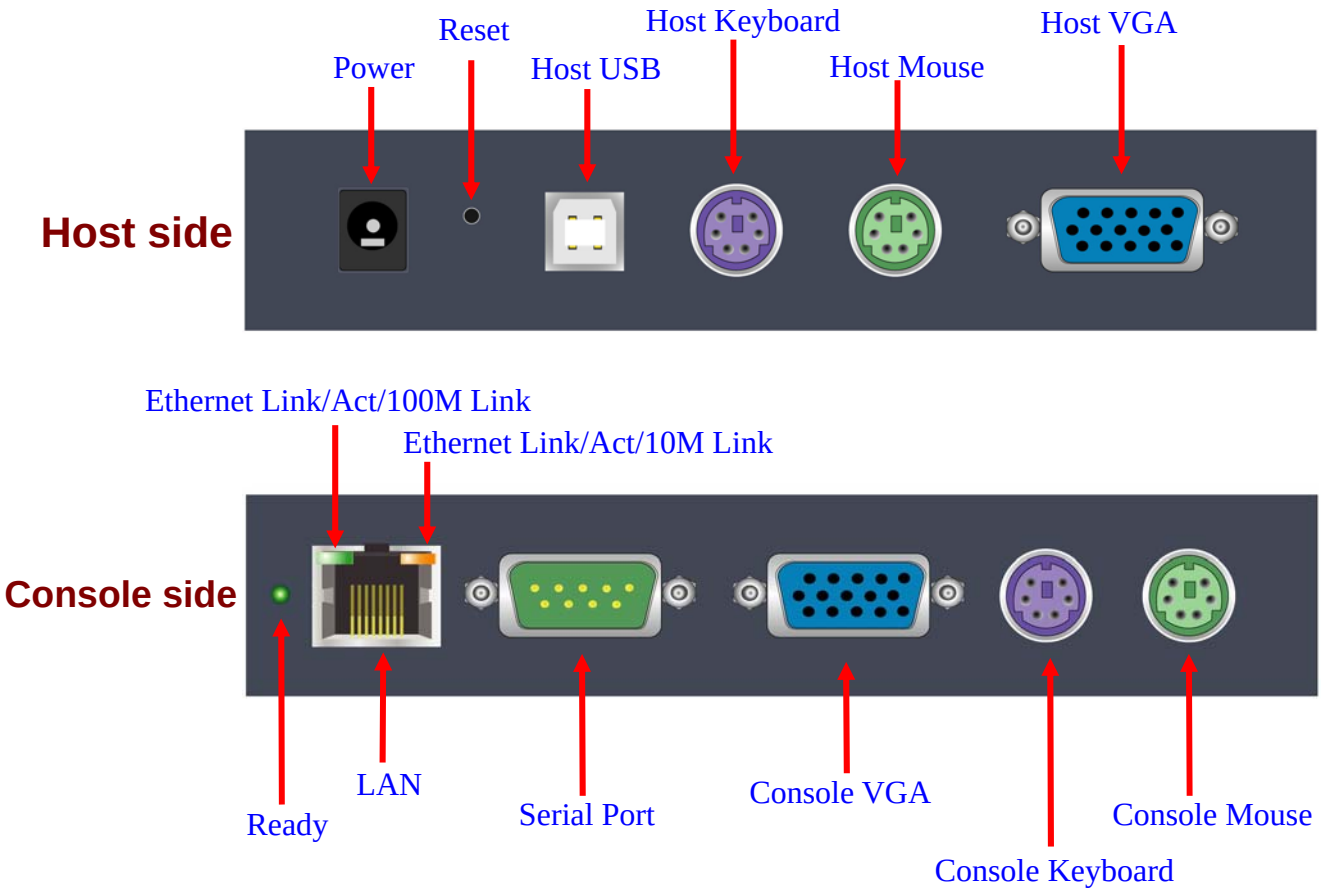
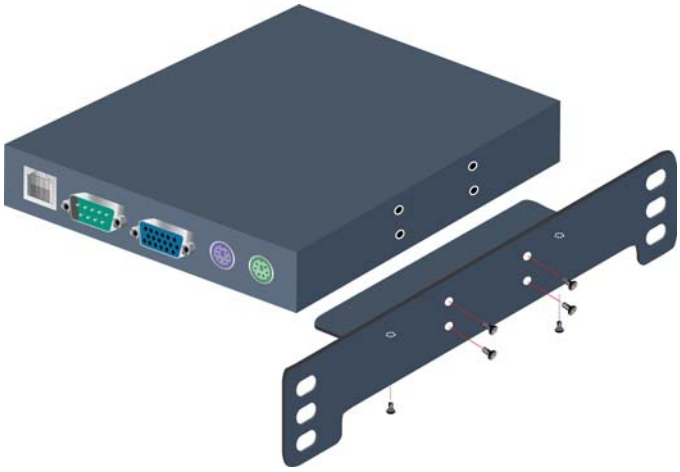


Figure 1 Panel Views

2.3 Rack Mounting

In addition to desk top placement, the IP-KVM can be mounted on 19”/1U rack:

1. Screw the mounting brackets into the sides of the unit, as shown in the diagram below.



2. Screw and secure the unit on the back side of the rack, so no take space of front rack.

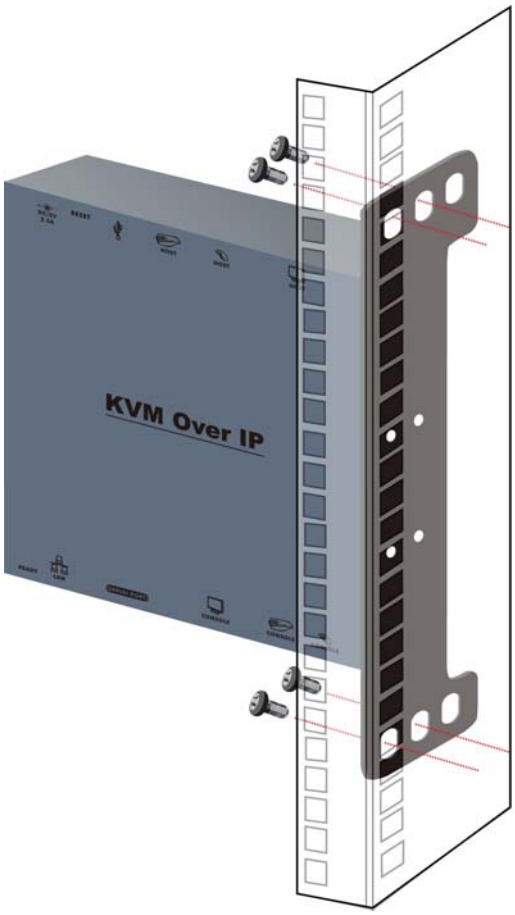


Figure 2 Rack Mount Installation

2.4 Cable Connections

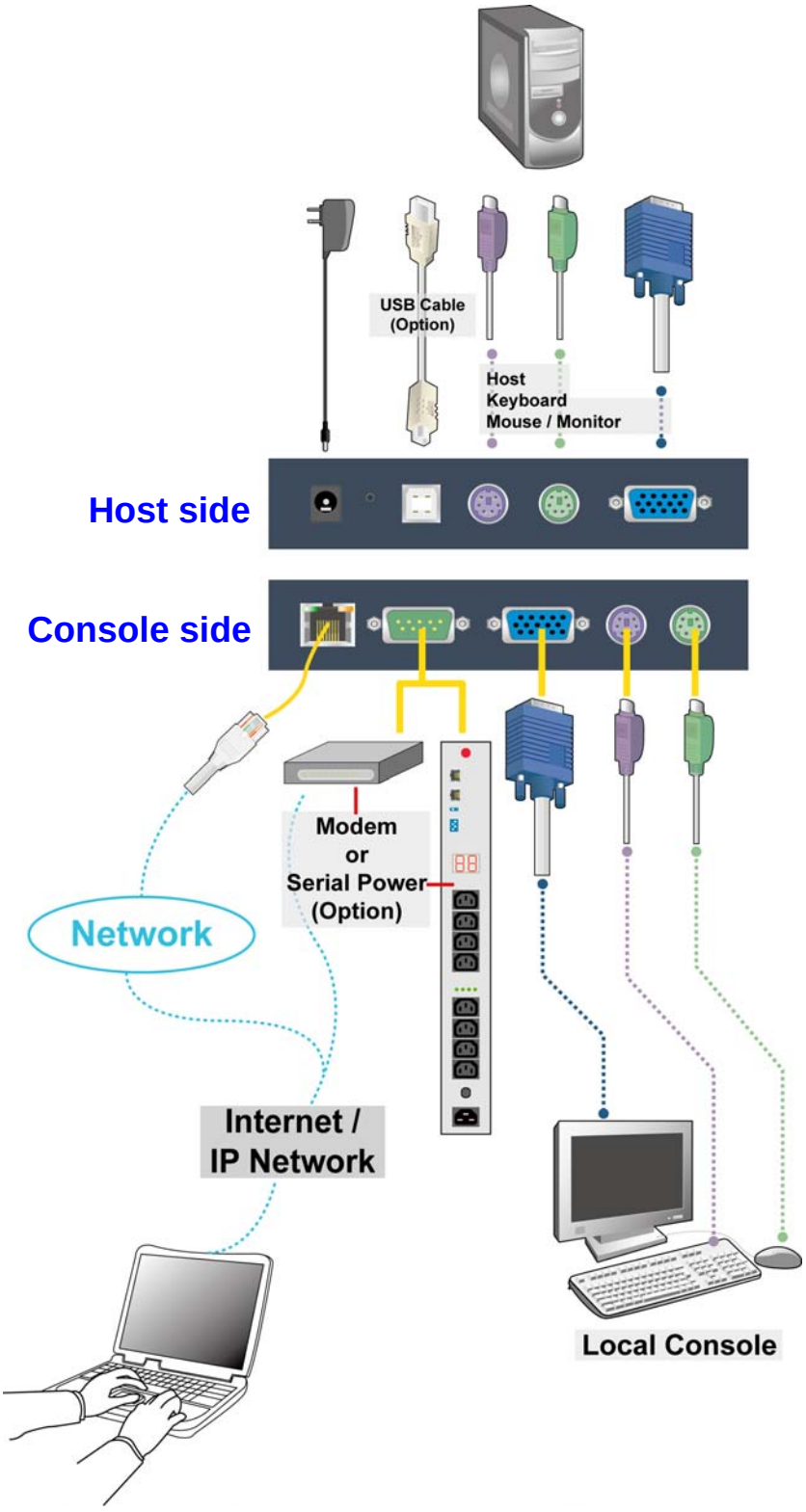


Figure 3 Cable Connections

Connect cables to the Host and Console devices as the figure depicts above. Leave the Serial interface open for now. After applying power to the unit, it'd take about 50 seconds to complete the bootup process. Then the READY LED will be blinking every second, meaning the unit has finished the startup and is running normally.

2.5 LED Indicators, Button

LED	Indication
LAN	**Ethernet Link/Act/10/100Mbps:** **Orange** -- 10BaseT Ethernet connection established **Green** -- 100BaseT Ethernet connection established *Blinking: when data in activity* *ON: when no data in activity and link connected*
Ready	**Green** -- blinking per second when system is ready

- **RESET** button: press the button to reboot the IP-KVM unit

2.6 Startup Guide

2.6.1 A Network Setup Software Tool -- IP Setup

In addition to VT100 interface, we also provide a Network Setup Software tool **(IP Setup)** for the network settings to the IP-KVM.

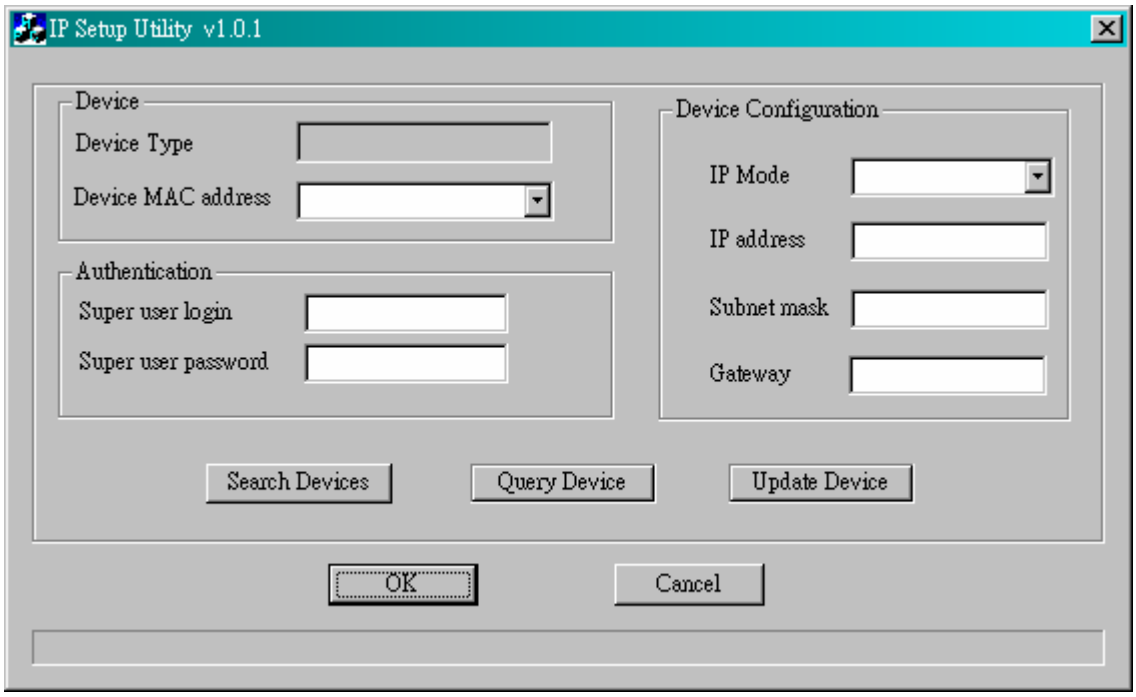
The Factory default settings for the IP-KVM unit are as below:

DHCP: Disable
Default IP address: 192.168.0.1
Default Net Mask: 255.255.255.0

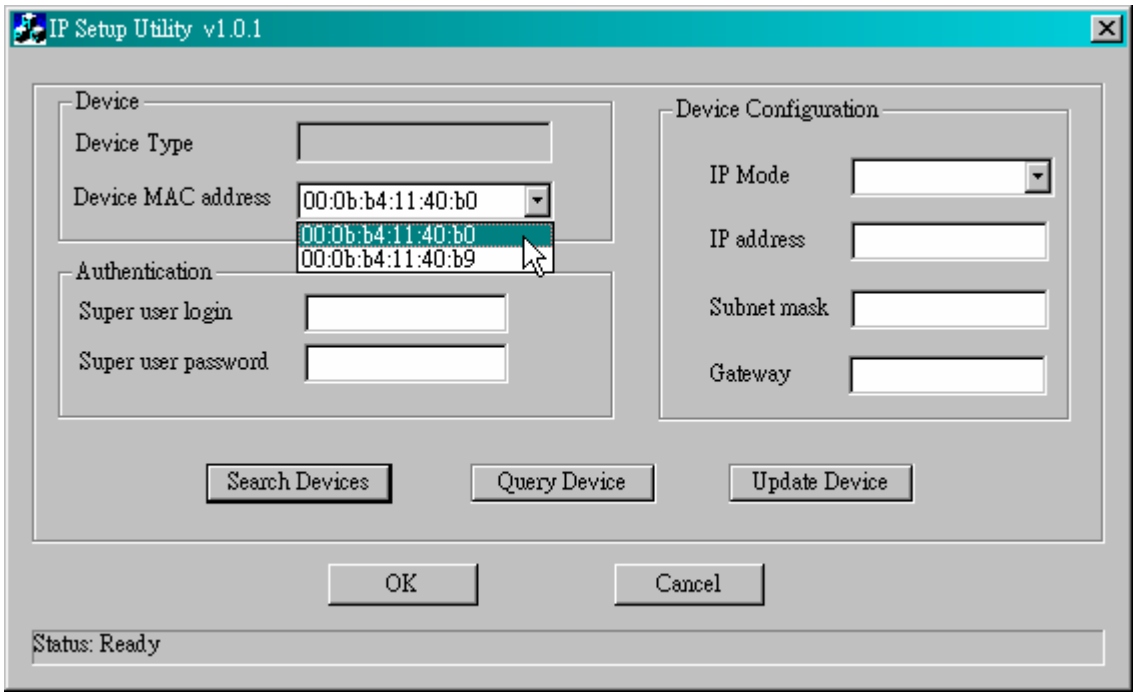
There is a Network Setup Software tool **(IP Setup)** for setting up the network configuration (IP address, Subnet mask, DHCP, etc). It is useful when you want to change the network settings or you can not access to the unit due to not knowing the network settings of the unit. In this case, you can view or change the settings via this utility.

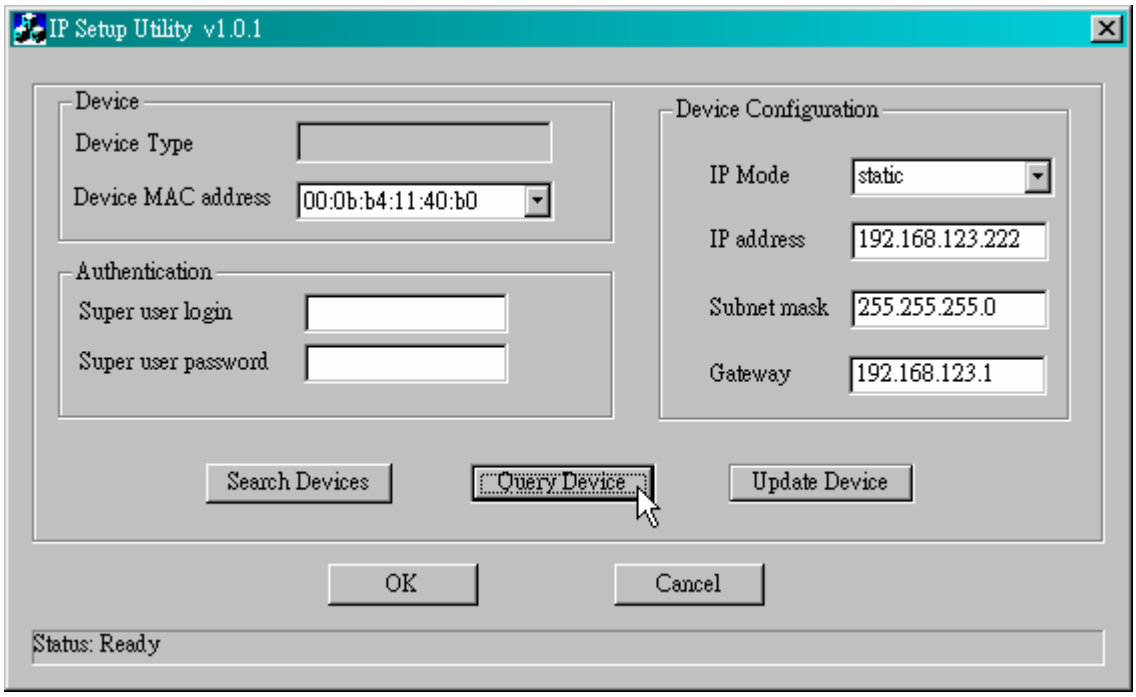
The operation procedures are as follows:

1. Run the software tool **IpSetup.exe**
2. Click **Search Devices** to find out the IP-KVM devices on the network. After few seconds, the MAC addresses of found devices will show on **Device MAC address** field.



3. Select the MAC address from **Device MAC address**, then click **Query Device** to get the device configuration on the right pane.





4. if you want to change the settings. Enter the Super user name & password. Change the settings on the right pane. Then click **Update Device.** The new settings will be saved to the IP-KVM unit, then the IP-KVM unit will reboot automatically.

3. Managements Overview

3.1 Access Privileges and Session Timeout

When connecting to the IP-KVM unit, the IP-KVM system (web server) will prompt user to enter the user name and password in order to access to the system.

The default user name and password are as follows.

Default User Name: root

Default Password: superuser

Note 1. The default user name and password are in lower-case characters.

Note 2. When you log in using the root user name and password, you have full administrative powers. It is advised that once you log in, you change the root password.

There are two levels of access privileges:

User Name	Default Password	Access Privileges
root	superuser	full access
(user define)	(user define)	limited access

The administrator can add or remove a user easily via the web pages of System administration.

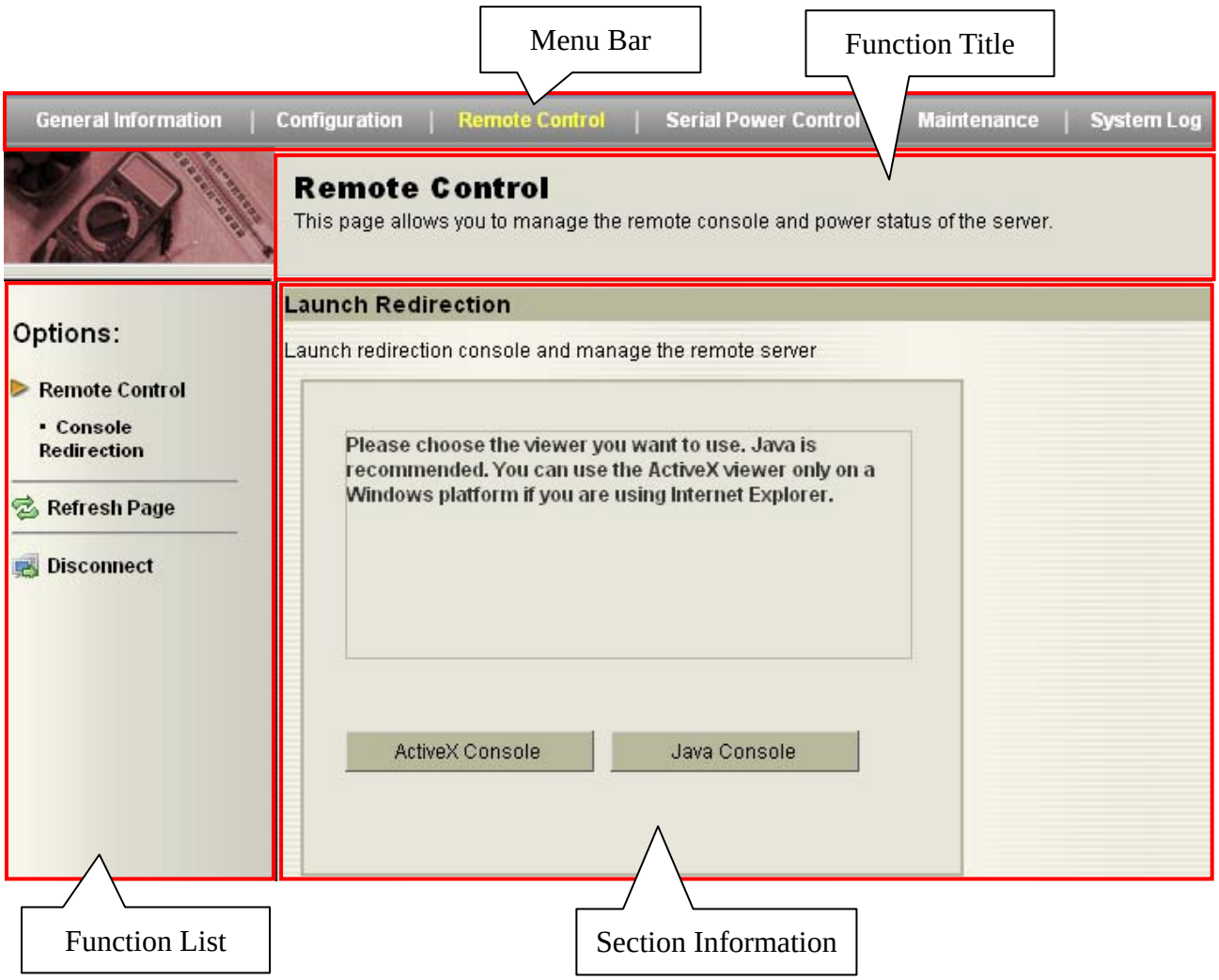
In order to protect IP-KVM system from unauthorized user access, a session access timeout of 5 minutes is fired or restarted each time the web page configuration is initiated. Users will be redirected to login webpage and asked to do account authentication again. The session timeout helps user to prevent from those who do not have access privilege to do system configuration. The login session will time out in 5 minutes and thus terminate the session to prevent others from accessing to IP-KVM system. The session timeout is reset if users keep working on the web configuration. The session timeout will be effective in case of they leave their web browser idle for 5 minutes.

3.2 Web Browser Management Interface

The IP-KVM supports both HTTP and HTTPS (HTTP over SSL) protocols. The users must authenticate themselves by logging into the system with a correct user name and password

To access the IP-KVM Web management pages, enter the IP-KVM unit's IP address or resolvable hostname into the web browser's URL/Location field. This will direct the user to the IP-KVM login screen.

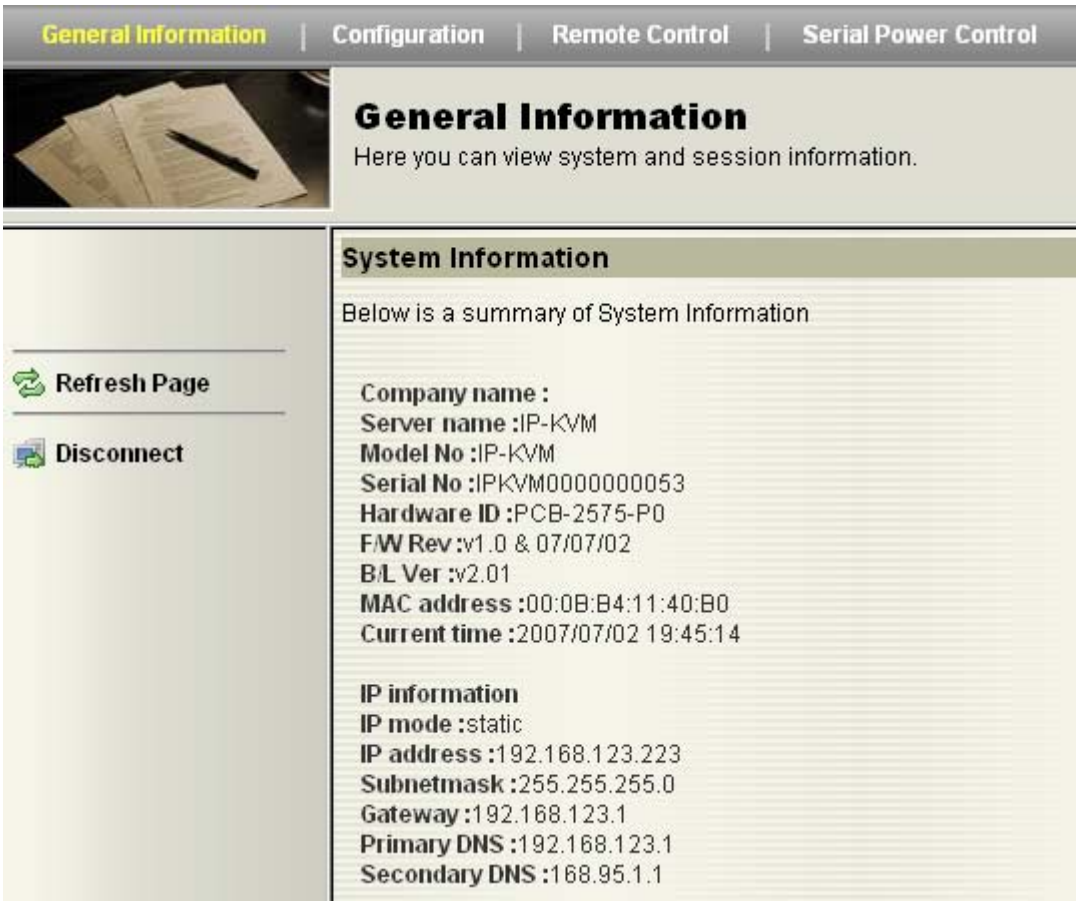
Figure below shows the user homepage of the IP-KVM Web management interface.



A menu bar displays on the top of the screen. Selecting an item on the menu bar opens a tree view of all the functions available under each grouping. Selecting a function item will allow the user to modify parameter settings for that item.

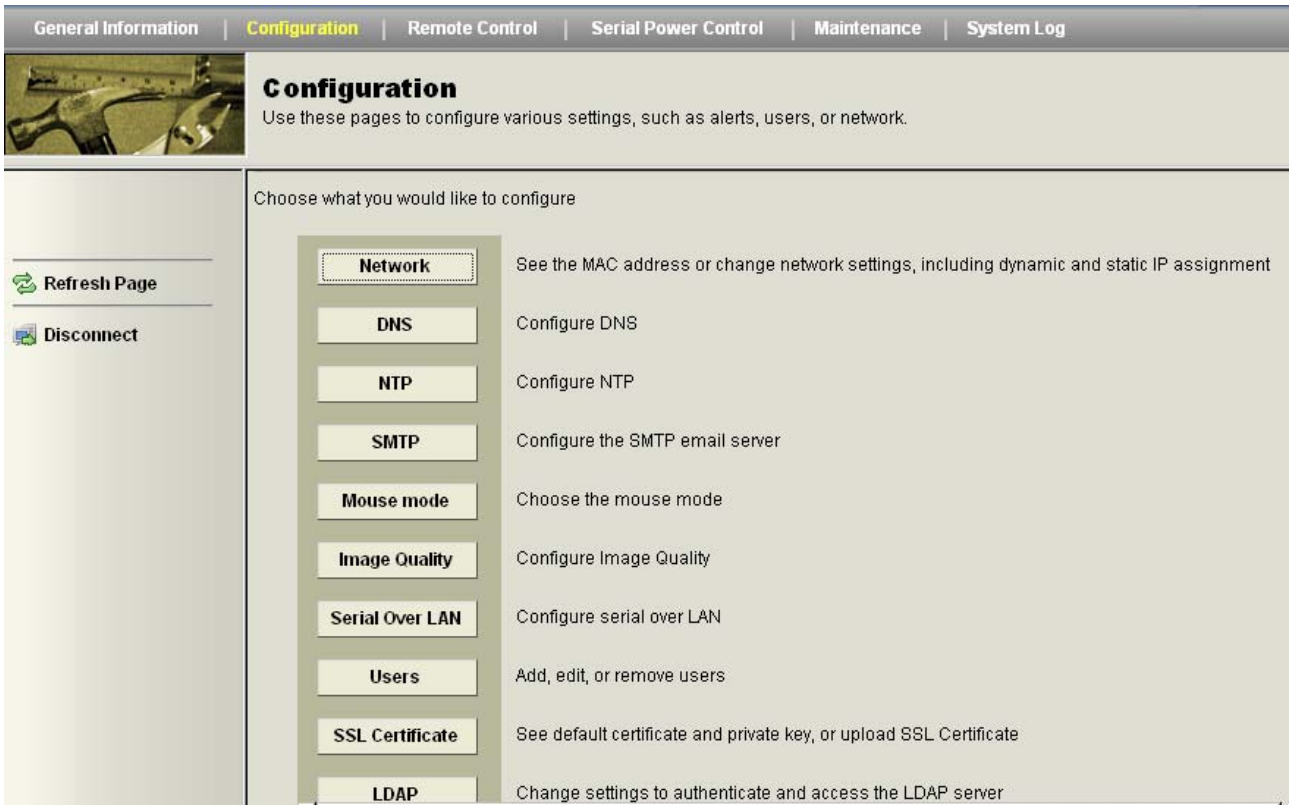
4. General Information

It lists the system information of the KVM over IP unit.



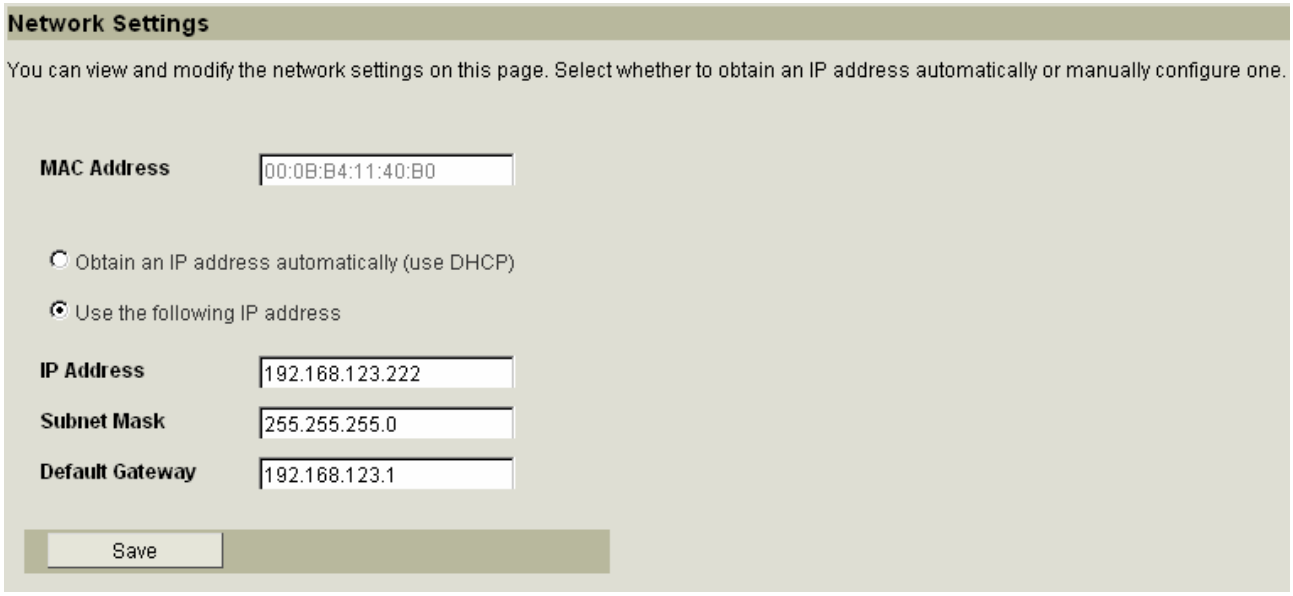
5. Configuration

Click **Configuration** to open the configuration list.


General Information | Configuration | Remote Control | Serial Power Control | Maintenance | System Log
Configuration
Use these pages to configure various settings, such as alerts, users, or network.
Choose what you would like to configure
Refresh Page
Disconnect
Network
See the MAC address or change network settings, including dynamic and static IP assignment
DNS
Configure DNS
NTP
Configure NTP
SMTP
Configure the SMTP email server
Mouse mode
Choose the mouse mode
Image Quality
Configure Image Quality
Serial Over LAN
Configure serial over LAN
Users
Add, edit, or remove users
SSL Certificate
See default certificate and private key, or upload SSL Certificate
LDAP
Change settings to authenticate and access the LDAP server

5.1 Network

The IP-KVM requires a valid IP address to operate within the user's network environment. If the IP address is not readily available, contact the system administrator to obtain a valid IP address for the IP-KVM. Please note that the IP-KVM requires a unique IP address to connect to the user's network.



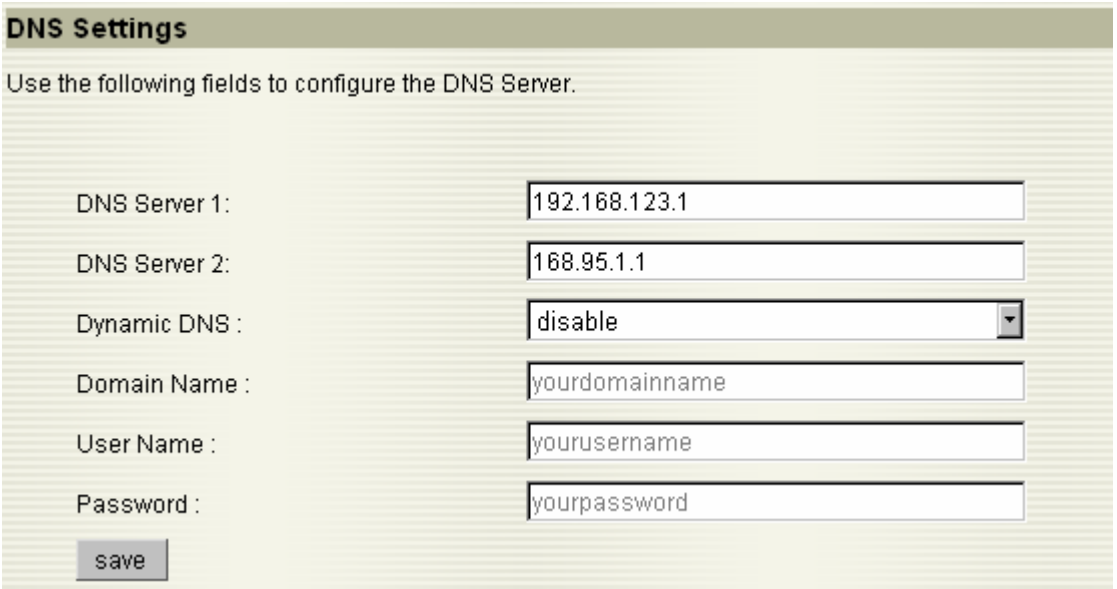
There are two types of IP assignments user can choose from:

- Static IP
- DHCP (Dynamic Host Configuration Protocol)

The IP-KVM is initially defaulted to Static IP mode, with a static IP address of 192.168.0.

The IP configuration setting will not go into effect until clicking the button **Save to flash & Reboot**.

5.2 DNS and Dynamic DNS



When users connect the IP-KVM to a DSL line or use a DHCP configuration, and get a dynamic IP address from the network, the IP address may not the same as previous. It can therefore be very difficult to know if an IP address has changed, or what the new IP address is.

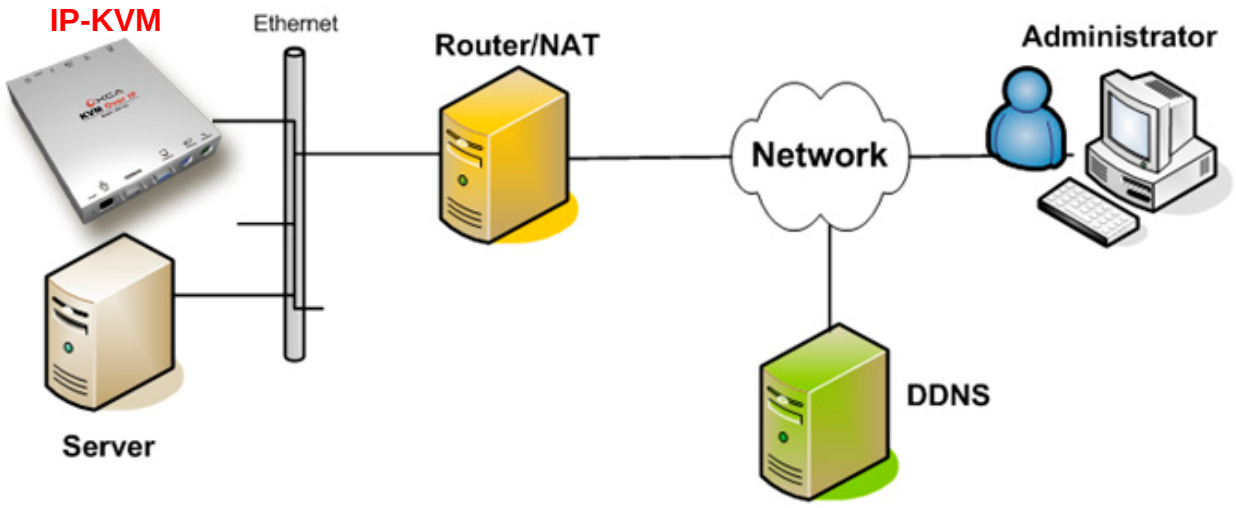


Figure 4 Dynamic DNS

A Dynamic DNS service is provided by various ISPs or organizations to deal with the above issue. By using the Dynamic DNS service, users can access the IP-KVM through the hostname registered in the Dynamic DNS Server regardless of any IP address change.
By default, the IP-KVM only supports Dynamic DNS service offered at Dynamic DNS Network Services, LLC (www.dyndns.org).

To use the Dynamic DNS service provided by Dynamic DNS Network Services, the user must set up an account in their Members' NIC (Network Information Center - http://members.dyndns.org). The user may then add a new Dynamic DNS Host link after logging in to their Dynamic DNS Network Services Members NIC.

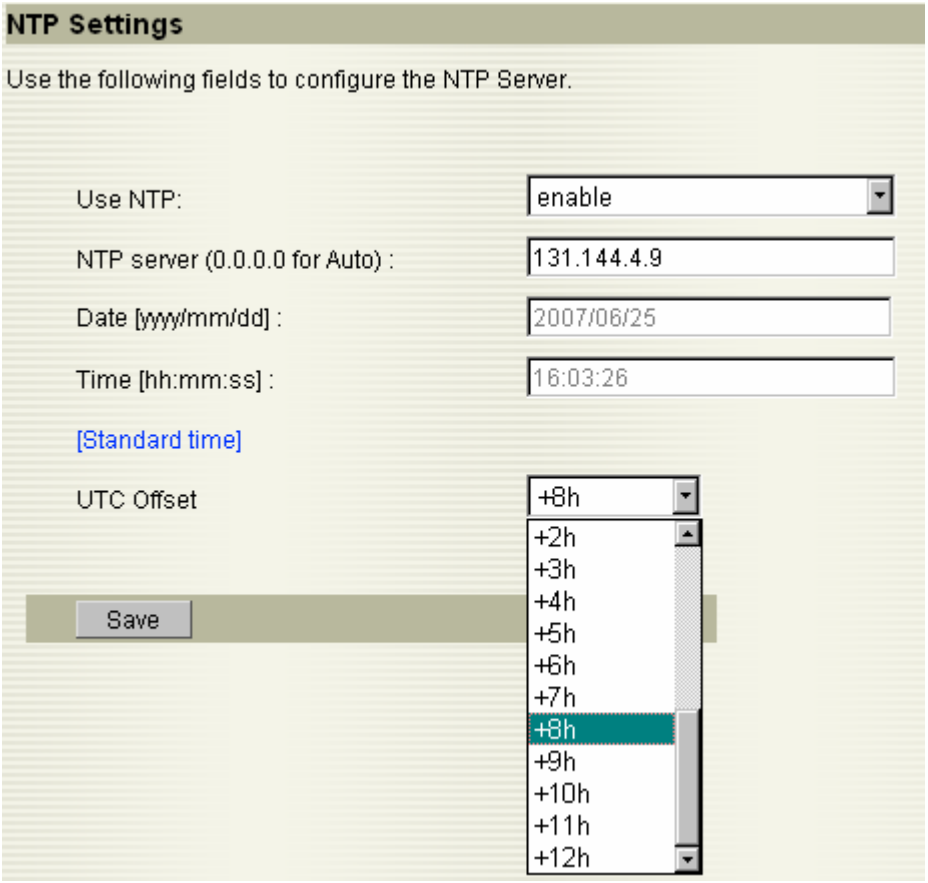
After enabling the Dynamic DNS service in the Dynamic DNS Configuration menu, the user must enter the registered Domain Name, User Name, and Password. After applying the configuration change, users can access the IP-KVM using only the Domain Name. The DNS (Domain Name Systems) is the internet service that translates your domain names into IP addresses.

5.3 NTP (Date and time)

The IP-KVM maintains current date and time information. The IP-KVM clock and calendar settings are backed up by internal battery power. The user can change the current date and time.

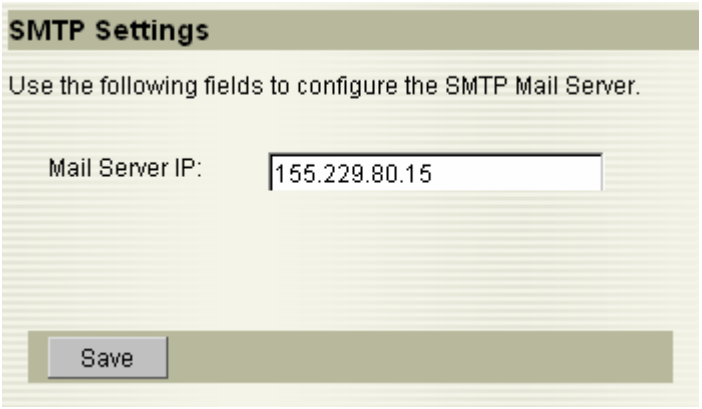
There are two methods of date and time settings. The first is to use the NTP server to maintain the date and time settings. If the NTP feature is enabled, the IP-KVM will obtain the date and time information from the NTP server at each reboot, then automatically align with the NTP server time per hour. If the NTP server is set to 0.0.0.0, the IP-KVM will automatically use the default NTP servers. In this case, the IP-KVM should be connected from the network to the Internet. The second method is to set date and time manually without using the NTP server. This will allow the date and time information to be kept maintained by the internal battery backup.

By convention, weather scientists use one time zone, Greenwich Mean Time (GMT). This time is also known as Universal Time (UTC). The user may also need to set the time zone and the time offset from UTC depending on the user location to set system date and time exactly, and the time offset from UTC. It allows the IP-KVM to calculate the exact system time. The **Time offset** value **x** could be positive or negative integer. Please refer to the website http://time_zone.tripod.com/ for the time offset from UTC.

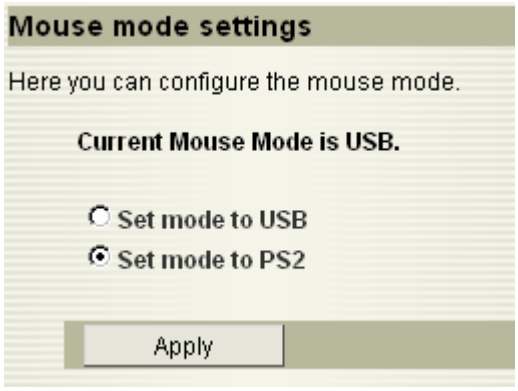


5.4 SMTP

The IP-KVM can send an email notification when the number of system log messages reaches to certain value and/or when an alarm message is created due to an issue with serial port data. The user must configure a valid SMTP server to send these automatically generated emails.
The “device mail address” must be registered to SMTP server.



5.5 Mouse Mode

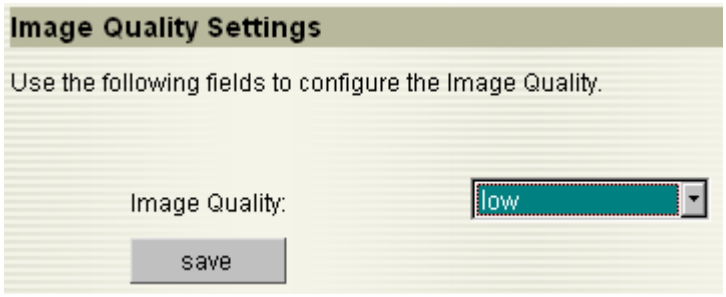


To select the mouse mode of host computer: USB or PS/2. Default is USB mode.

Note: please set the mode properly, or the RC (Remote Control) function won't work.

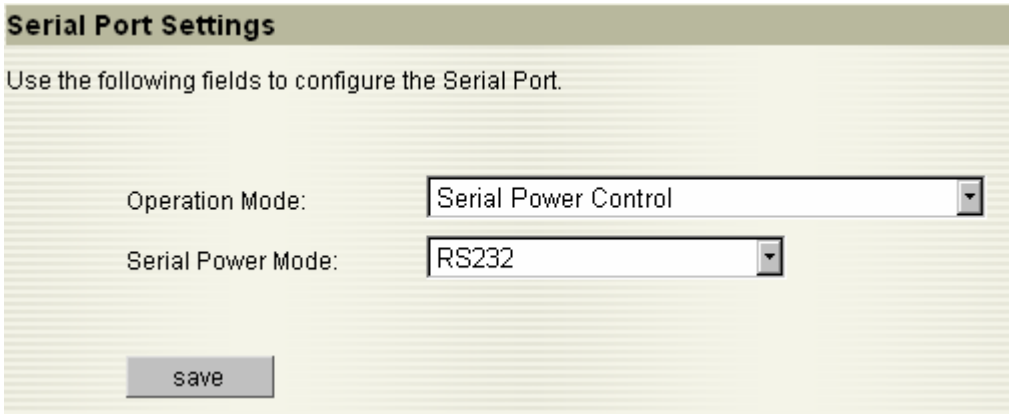
5.6 Image Quality

To select the video image quality. There are three levels to select: low, medium, and high.
Note: higher quality will return lower frame rate. User can choose the level to suit his/her application.

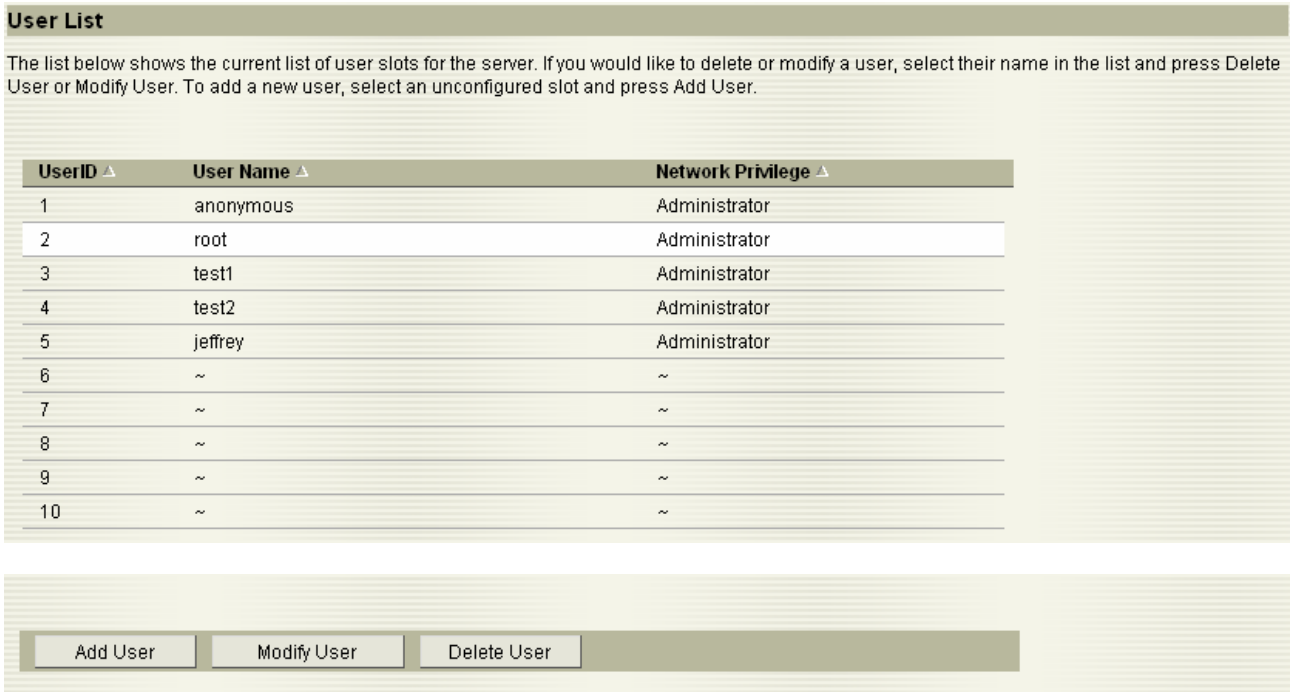


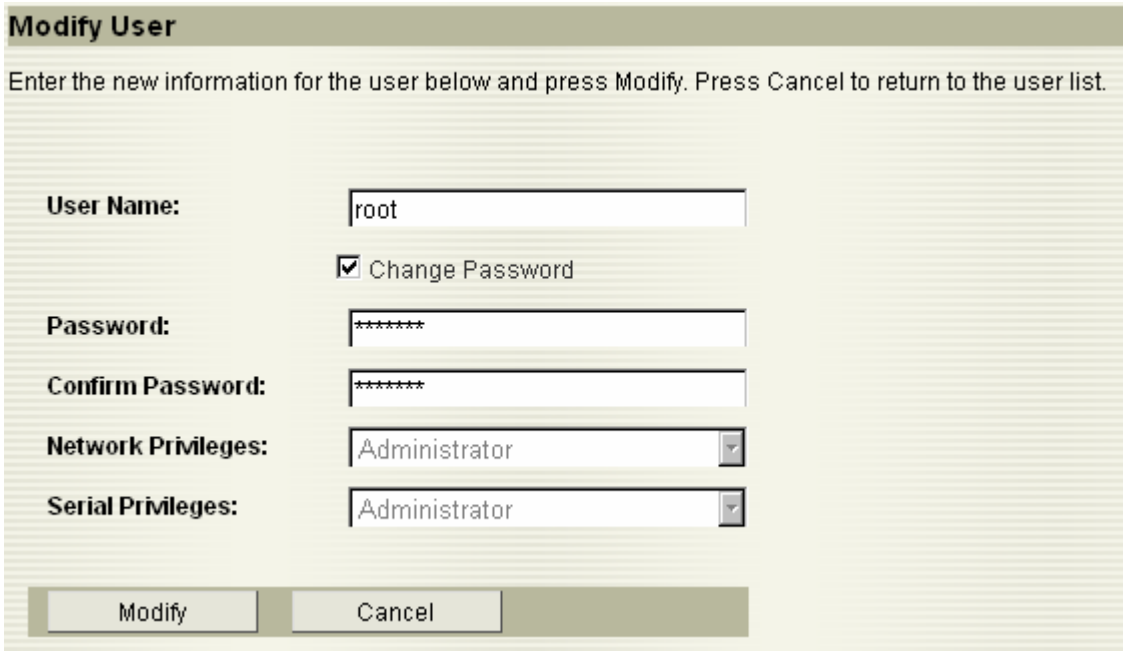
5.7 Serial over LAN

To select the serial port function: Serial Power Control or Remote Console Server (will provide in next FW release).



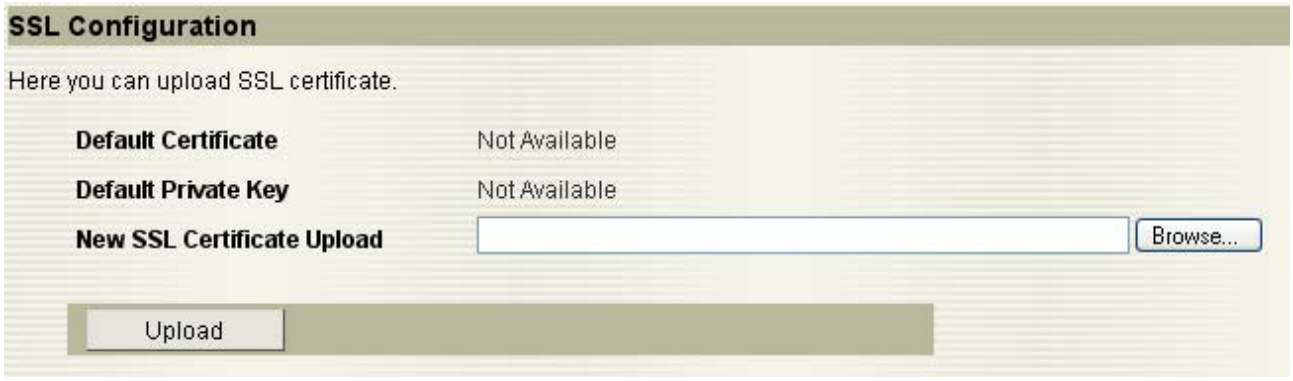
5.8 Users


User List
The list below shows the current list of user slots for the server. If you would like to delete or modify a user, select their name in the list and press Delete User or Modify User. To add a new user, select an unconfigured slot and press Add User.
UserID
User Name
Network Privilege
1 anonymous Administrator
2 root Administrator
3 test1 Administrator
4 test2 Administrator
5 jeffrey Administrator
6 ~ ~
7 ~ ~
8 ~ ~
9 ~ ~
10 ~ ~
Add User
Modify User
Delete User



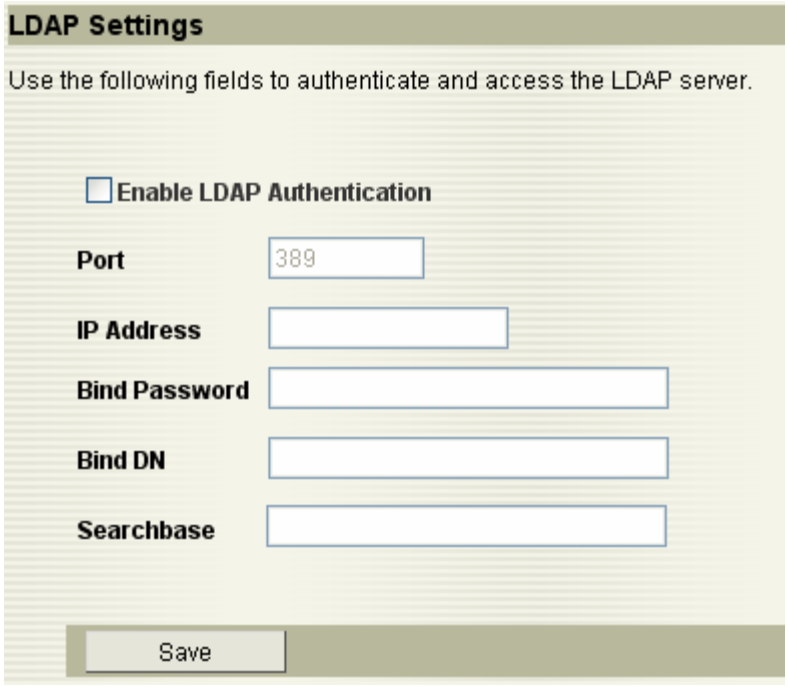
5.9 SSL Certificate

To upload the SSL file to the server (KVM over IP).



5.10 LDAP

It can download user list of LDAP server then create user account from this list directly.



6. Remote Control

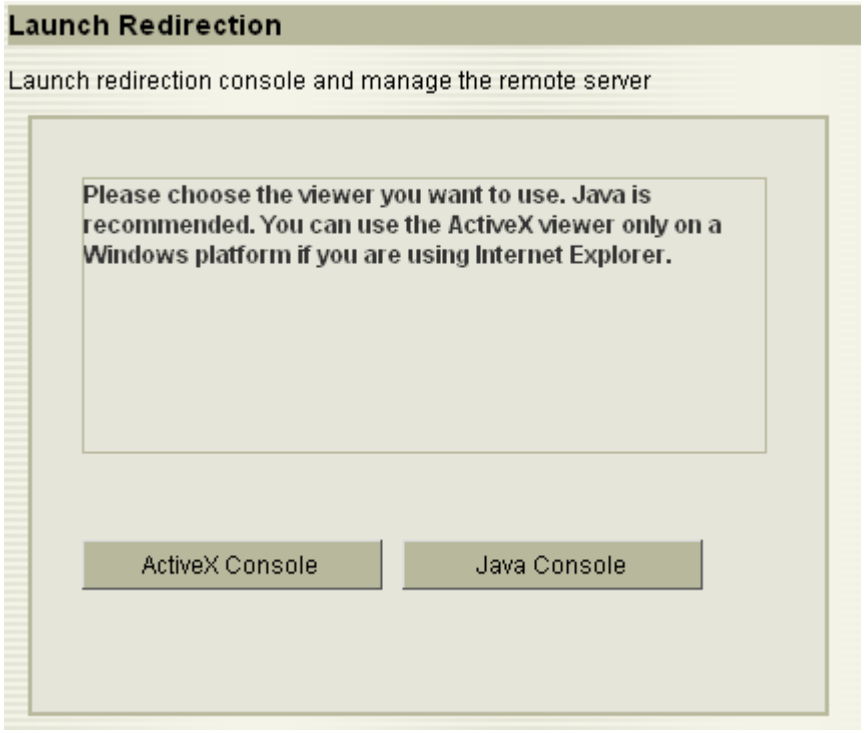
6.1 Remote KVM Console

The most powerful feature of your IP-KVM is the ability to redirect the host system's console. To redirect the host system's console is the ability to manage your host system as if it were physically in front of you, but not.
This menu item allows you to start a Remote Console session with the host system.
Launch Redirection: There have two modes for console redirection:

- JAVA Console for Mazila or FireFox (for Linux client machine).
- ActiveX Console for IE Browser (for Windows client machine). This mode needs to enable all ActiveX items of IE Browser.

Click **Remote Control** on the Menu bar.

Click **Console Redirection**

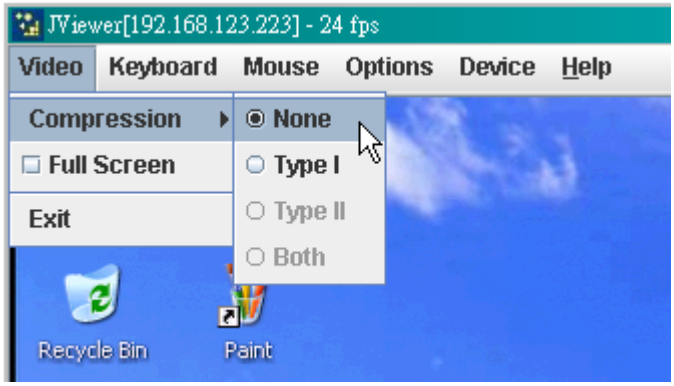

Launch Redirection
Launch redirection console and manage the remote server
Please choose the viewer you want to use. Java is recommended. You can use the ActiveX viewer only on a Windows platform if you are using Internet Explorer.
ActiveX Console
Java Console

There are two types of remote KVM redirection software: ActiveX or Java.
Java is recommended. You can use ActiveX on a Windows platform and using IE.

> **Notes:**
> In order to run this function, the system need support J2RE (Java 2 Runtime Environment) 1.5 and above, or Sun ™ JRE(Java Runtime Environment) 5.0 and above. You can get the Java Software from the website http://www.java.com/en/download/

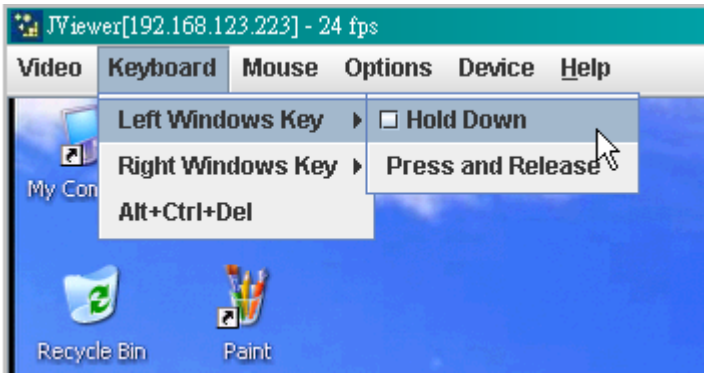
Click **OK** on the Security Warning. The RC (remote console) will show up as below.

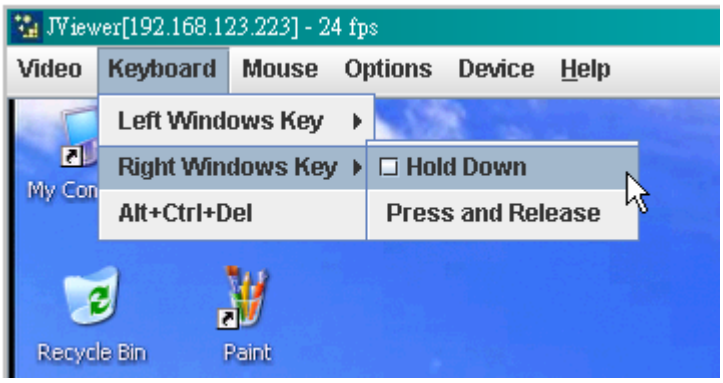
The **Video** settings on the menu bar of RC (remote console):



Compression	This menu item can be chose modes for compress video signal: # None: default setting. Use hardware compressing engine. For wide bandwidth internet. # Type-I: Level 1 software compressing engine. For xDSL/Cable Modem. # Type-II: Level 2 software compressing engine. For xDSL/Cable Modem. # Both: Use Level 1 and 2 software compressing engine. For 56K Modem.
Full Screen	This menu item can be used to view the *Console Redirection* in *Full Screen* mode. Note: Set your client system's screen resolution to 1024 x 768 so that you can view the host system in true full screen.
Exit	Exit console redirection.

The **Keyboard** settings on the menu bar of RC (remote console):



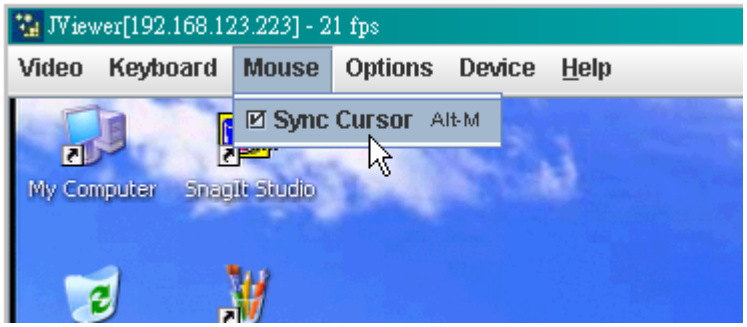


Left Windows Key	This menu item can be used to access the left-side <WINDOWS> key during a Console Redirection session. The following actions can be performed: - *Hold Down* - *Press and Release*
Right Windows Key	This menu item can be used to access the right-side <WINDOWS> key during a Console Redirection session. The following actions can be performed: - *Hold Down* - *Press and Release*
ALT+CTRL+DEL	This menu item can be used to act as if you depressed the <CTRL>, <ALT> and <DEL> keys down simultaneously on the host system that you are redirecting.

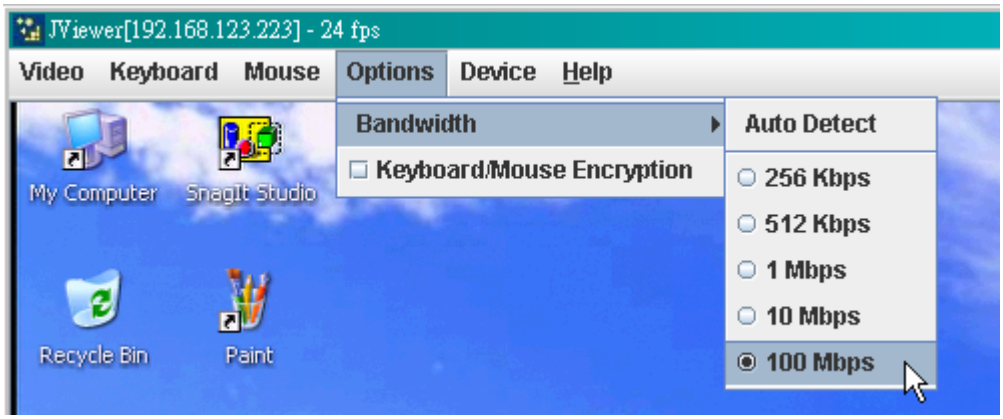
The **Mouse** settings on the menu bar of RC (remote console):

Sync Cursor for remote control mouse, **to bring the mouse cursor in or out of RC**.

The hotkey **Alt+M** is especially useful when trying to get the mouse out of RC.

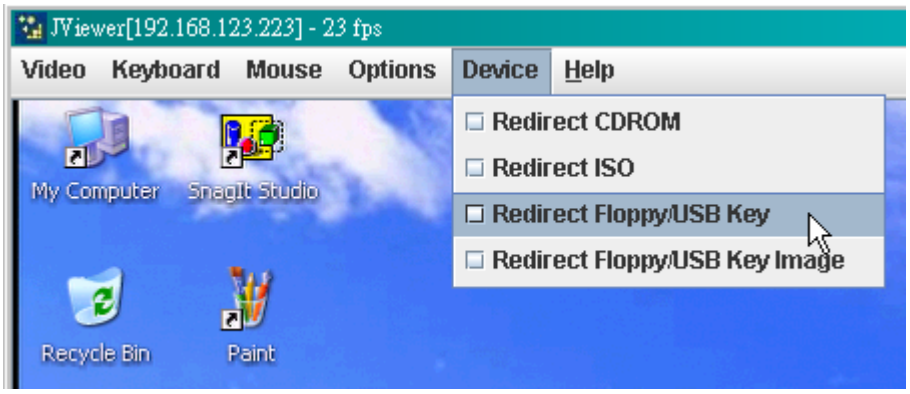


The **Options** settings on the menu bar of RC (remote console):



Bandwidth	To regulate the network bandwidth
Keyboard/Mouse Encryption	To encrypt the keyboard/mouse signal

The **Device** settings on the menu bar of RC (remote console): Virtual Device for remote control.

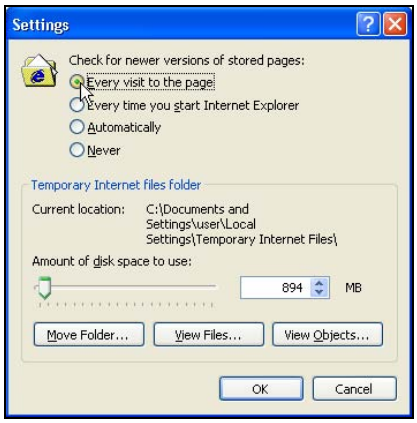


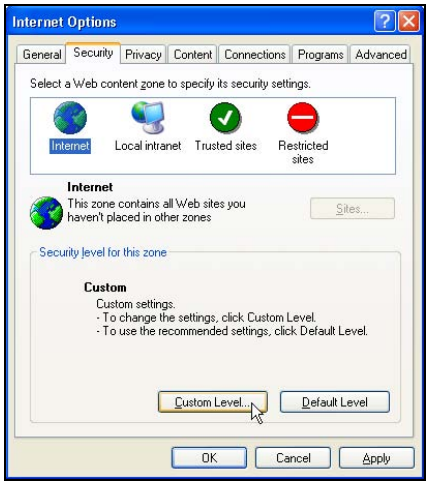
CDROM	This menu item can be used to start or stop the redirection of the CD-ROM drive.
ISO	It can be chose the CD Image file or CD-ROM drive from client computer.
Floppy/USB	This menu item can be used to start or stop the redirection of the floppy or USB drive.
Floppy/USB Image	It can be chose the Floppy or USB Image file from client computer.

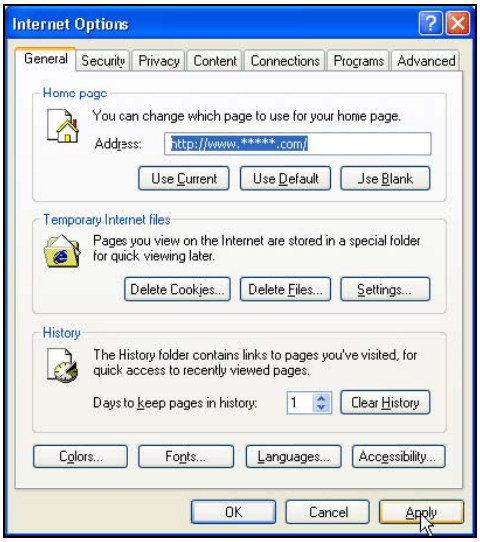
6.2 Special Settings for ActiveX

Setting up Internet Explorer

You must first setup your Internet browser before you can redirect the host system's console.

Step	Description
1	**Open *Internet Options*. To get there, open your Internet Explorer browser, left click *Tools* and then *Internet Options*.**
2	**The *Internet Options* window opens. Left click the *Settings* button.**
3	**The *Settings* window opens. Left click the *Every visit to the page* button or *Automatically* button. Left click the *OK* button to apply the change and to go back to the *Internet Options* window.**  **Note:** Other settings can cause old data to be displayed when performing operations on the IPKVM

4	**Next, you must setup Internet Explorer to allow the downloading of Signed ActiveX controls and also allow it to run Signed ActiveX controls. To do this, left click the *Security* tab and then the *Custom Level* button.**  **Note:** In Microsoft Windows 2003 server operating systems, the default security setting is *High*, and this disables many items (besides the Active X ones mentioned in this document) that are necessary to even access the IPKVM GUI. The security settings for a Microsoft Windows 2003 server operating system remote client must be on *Medium* or *Low*.
5	**The *Security Settings* window opens. Left click the *Enable* button under the *Download signed ActiveX controls* section.**

6	**Scroll down and left click the *Enable* button under the *Run ActiveX controls and plug-ins* section. Left click the *OK* button.**
7	**You are prompted with a *Warning* window. Left click the *Yes* button to accept the changes to the Internet zone and to go back to the *Internet Options* window.**
8	**Left click the *Apply* button and then the *OK* button to make the changes.**  **Note:** You must restart Internet Explorer before the changes take effect. **Note:** *Remote Console* cannot run with any other security settings in Internet Explorer.

7. Serial Power Control

The **Serial Power Controller (SPC)** is a family of intelligent power distribution units that enables remote power control of servers and network appliances. When used in conjunction with IP Console Servers, the SPC provides comprehensive management capabilities and quick problem resolution by integrating console access with power control into a single interface.

The SPC support both RS232 and RS485 interface. With RS485 mode, the SPC can be located up to 1.2km away from the controlling master, and has the Daisy- chain capability.

For detailed operation, please refer to the **User Manual of Serial Power Controller**.

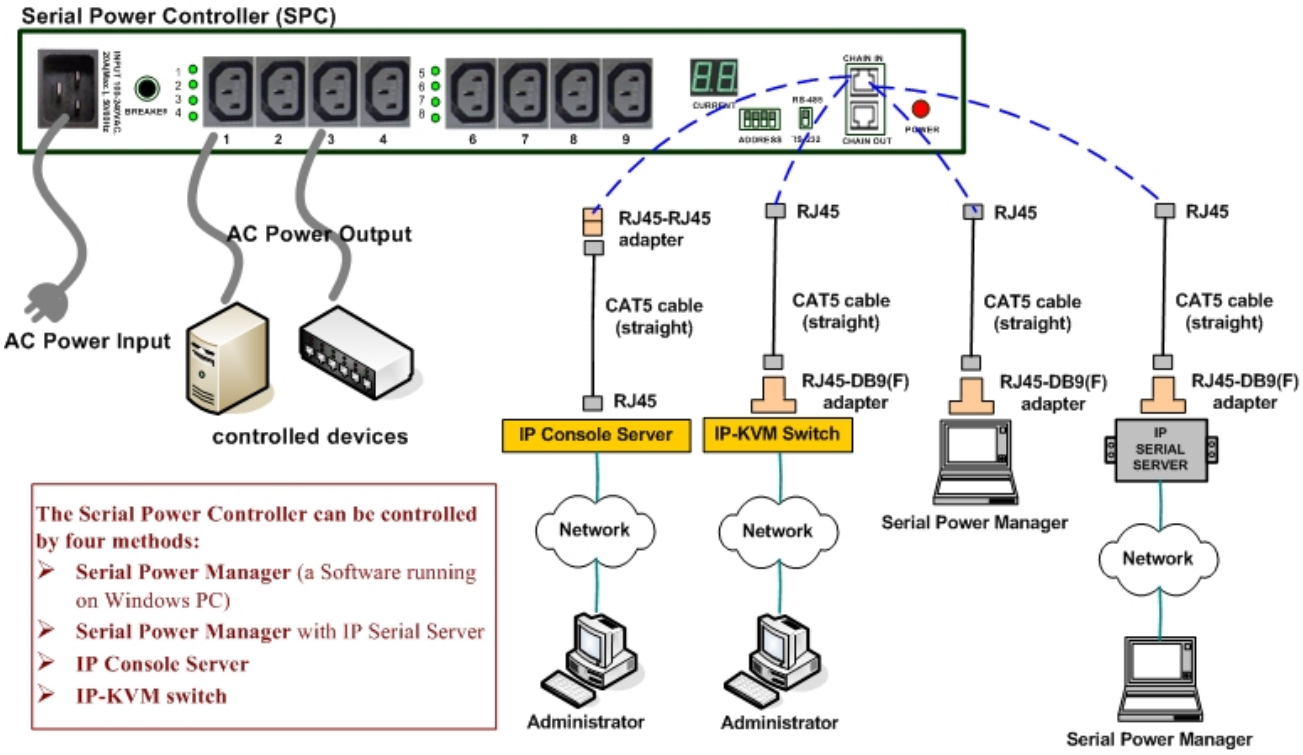


Figure 5 Serial Power Control

8. Maintenance

8.1 Firmware Upgrade

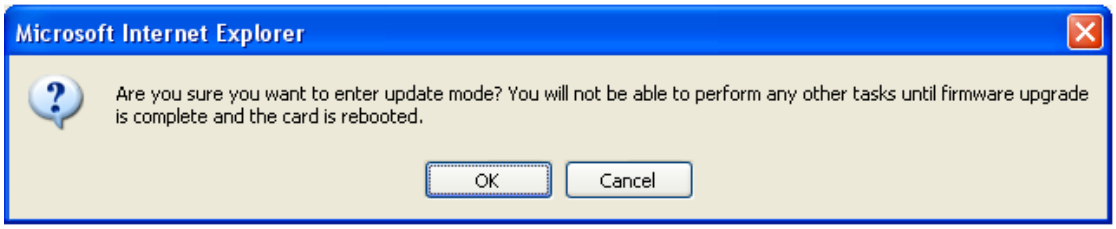
Firmware can be easily upgraded via web page. This section describes the upgrade procedures.

8.1.1 Upgrade from web page

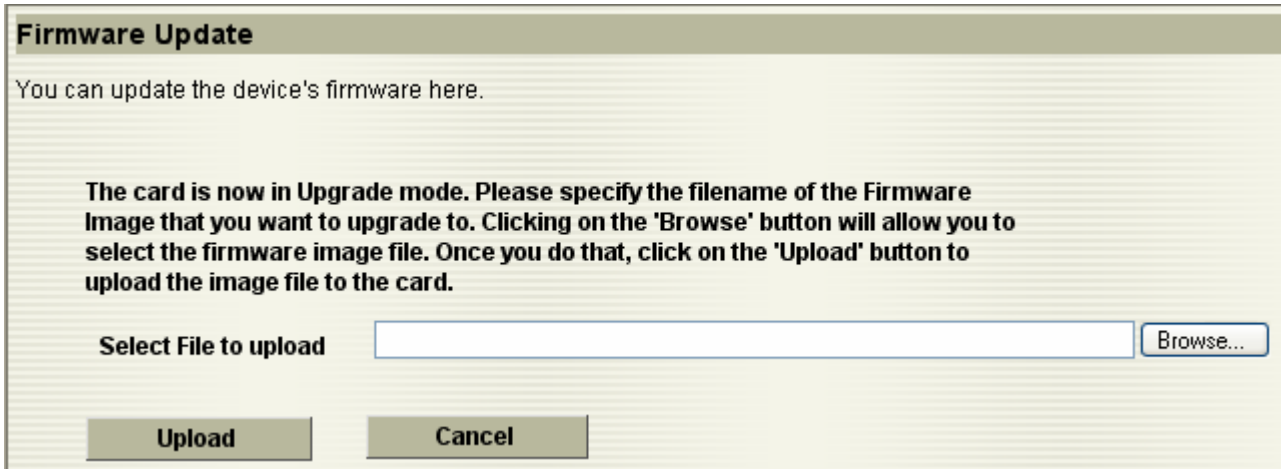
Select **Maintenance** from the Menu Bar.

Configuration
Remote Control
Maintenance
Languages
Maintenance
This page allows you to do maintenance tasks on the device.
Firmware Update
You can update the device's firmware here.
Press enter update mode to put the device in a special mode that allows firmware update. The device will reset if update is canceled.
Enter Update Mode

Click **Enter Update Mode**.

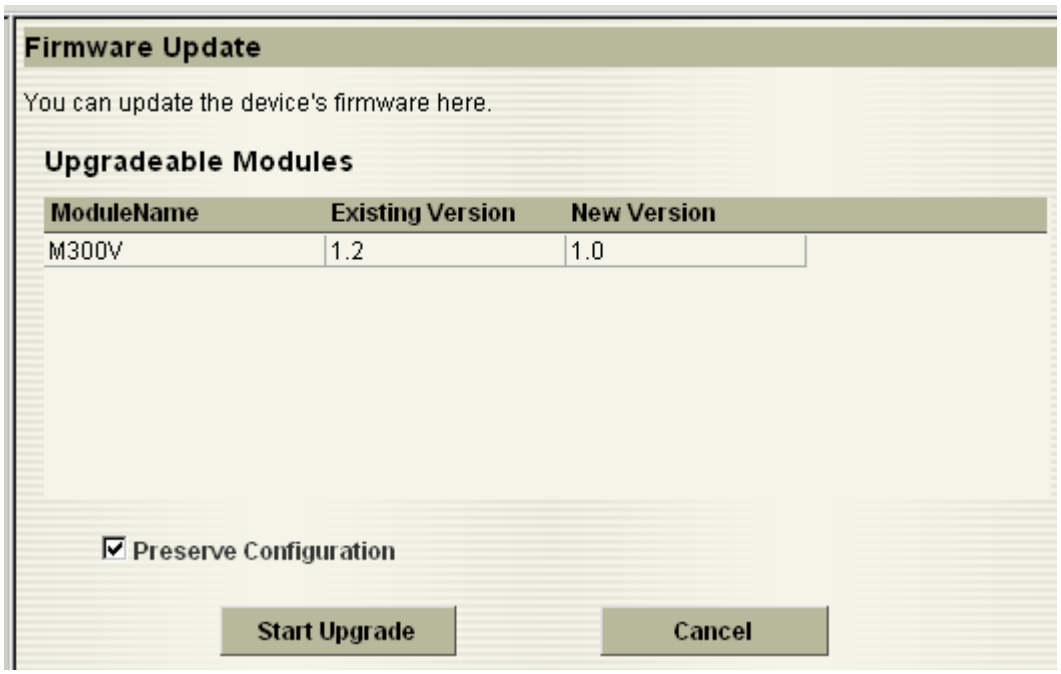

Microsoft Internet Explorer
Are you sure you want to enter update mode? You will not be able to perform any other tasks until firmware upgrade is complete and the card is rebooted.
OK
Cancel

Click **OK**.

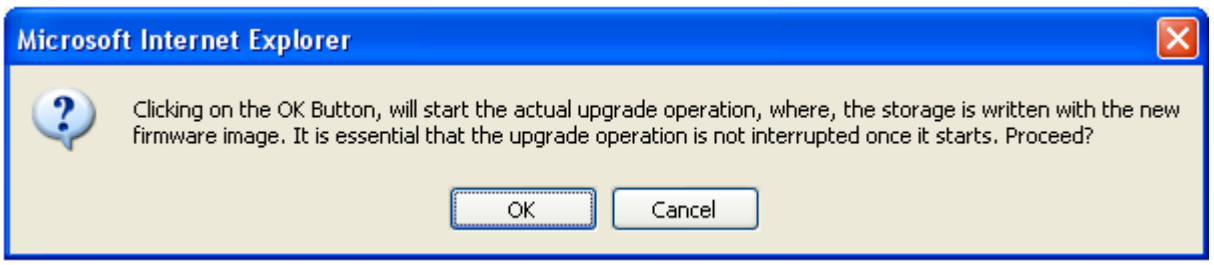

Firmware Update
You can update the device's firmware here.
The card is now in Upgrade mode. Please specify the filename of the Firmware Image that you want to upgrade to. Clicking on the 'Browse' button will allow you to select the firmware image file. Once you do that, click on the 'Upload' button to upload the image file to the card.
Select File to upload
Browse...
Upload
Cancel

Click **Browse** and select the file of the firmware image that you want to upgrade to.

Click **Upload** to upload the image file to the IP-KVM.

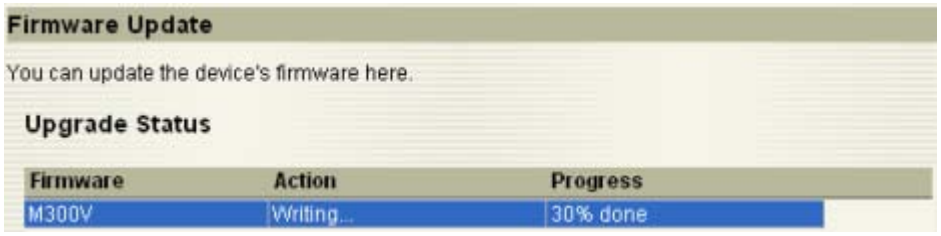


Click **Start Upgrade**.

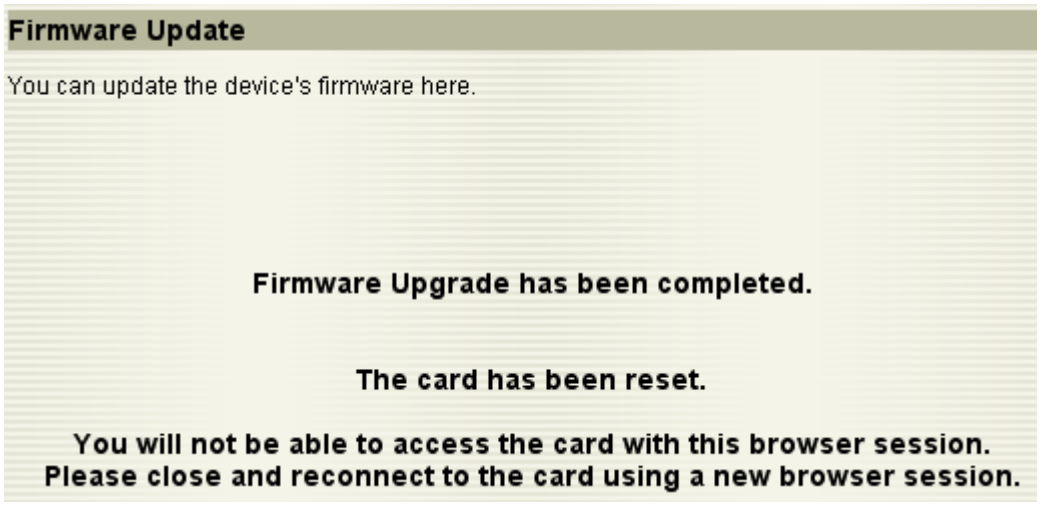

Microsoft Internet Explorer
Clicking on the OK Button, will start the actual upgrade operation, where, the storage is written with the new firmware image. It is essential that the upgrade operation is not interrupted once it starts. Proceed?
OK
Cancel

Click **OK.**

Warning !!!
During this upgrading process, we should not disconnect the power or the Ethernet cable, since it may cause upgrade failure and destroy the image in Flash memory. In this case, we have to upgrade though bootloader process, which is not as friendly as the web method.



After a few seconds, the message **Firmware Upgrade has been completed** will be shown, meaning the new firmware has been upgraded into the Flash memory.


Firmware Update
You can update the device's firmware here.
Firmware Upgrade has been completed.
The card has been reset.
You will not be able to access the card with this browser session.
Please close and reconnect to the card using a new browser session.

If you want to run the new firmware, you need to click the **Reboot** item, then **Yes** to confirm to reboot the system. It will take about one minute to finish the system reboot. When the IP-KVM unit finishes the startup and working normally, the Ready green LED will blink every second.

After a few seconds, the message **Flash program finished successfully** will be shown, meaning the new firmware has been upgraded into the Flash memory.

Warning !!!
During this upgrading process, we should not disconnect the power or the Ethernet cable, since it may cause upgrade failure and destroy the image in Flash memory. In this case, we have to upgrade though bootloader process, which is not as friendly as the web method.

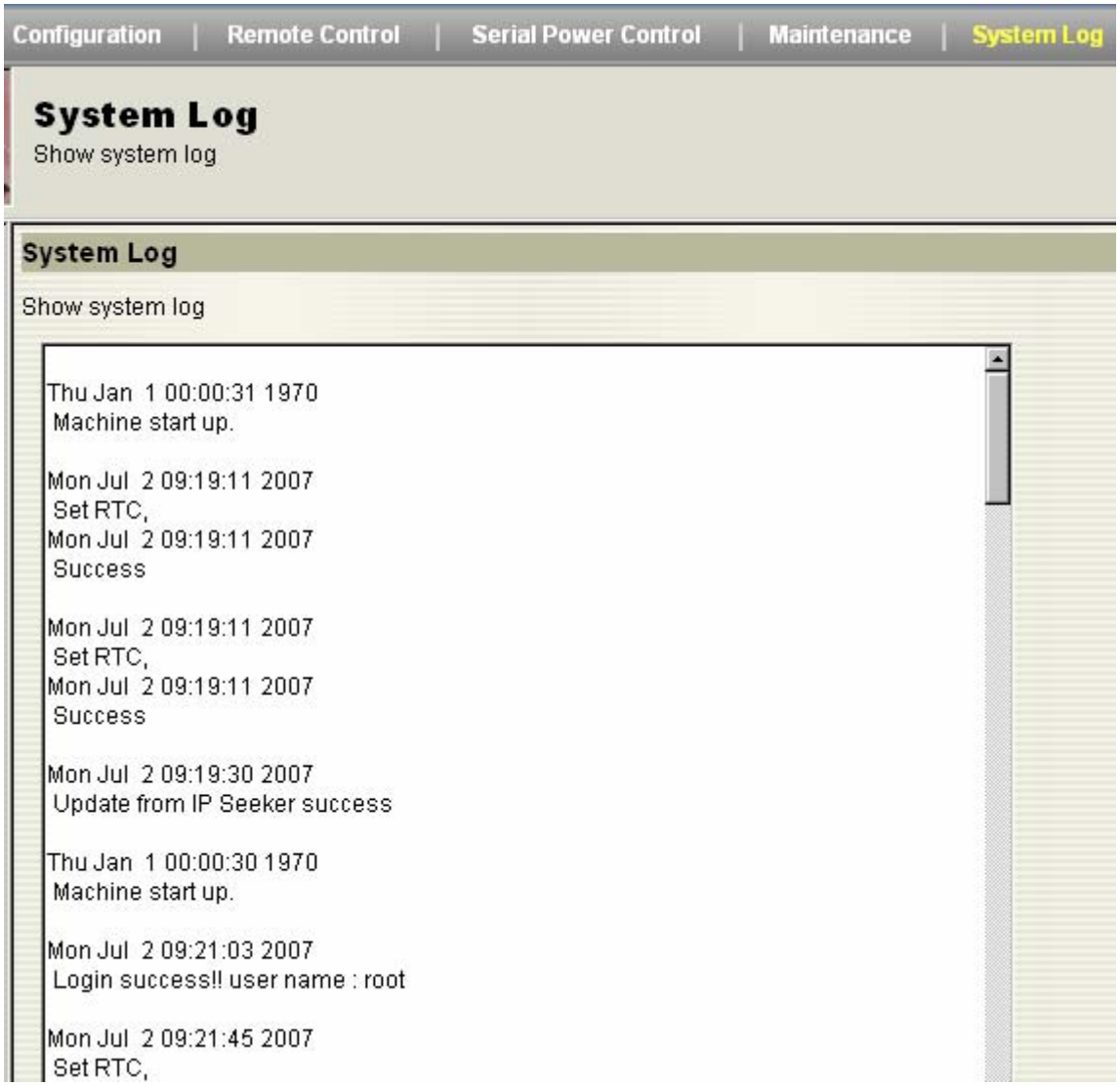
If you want to run the new firmware, you need to click the **Reboot** item, then **Yes** to confirm to

reboot the system. It will take about one minute to finish the system reboot. When the IP-KVM unit finishes the startup and working normally, the Ready green LED will blink every second.

Warning !!!
A new firmware release version may need one, two, or up to three images to upgrade. **You have to upgrade all to-be upgraded images before rebooting the system.** Otherwise may cause inconsistency between kernel and application firmware and the system may not be able to start up successfully. In this case, we have to upgrade though bootloader process, which is not as friendly as the web method.

9. System Log

The log function will log the system operation, like login activity, no matter fail or success.
The system log buffer is pre-allocated at 300K bytes size. If the logging data grows larger than the pre-allocated size, the new data will overwrite the old data.


Configuration | Remote Control | Serial Power Control | Maintenance | System Log
System Log
Show system log
System Log
Show system log
Thu Jan 1 00:00:31 1970
Machine start up.
Mon Jul 2 09:19:11 2007
Set RTC,
Mon Jul 2 09:19:11 2007
Success
Mon Jul 2 09:19:11 2007
Set RTC,
Mon Jul 2 09:19:11 2007
Success
Mon Jul 2 09:19:30 2007
Update from IP Seeker success
Thu Jan 1 00:00:30 1970
Machine start up.
Mon Jul 2 09:21:03 2007
Login success!! user name : root
Mon Jul 2 09:21:45 2007
Set RTC,

10. Technical Data

10.1 Technical Specifications

Feature	Specification
Host Side	1x VGA HDDB 15-pin (female)
	2x PS/2 mini Din 6-pin for Keyboard and Mouse(female)
	1x USB 2.0 Type B
	1x Reset button
	1x Power Jack
Console Side	1x VGA HDDB 15-pin (female)
	2x PS/2 mini Din 6-pin for Keyboard and Mouse(female)
	1x Standard RJ-45 Connector for LAN port
	1x DB9 (male) for Serial port
	1x Green LED (READY)
Max. Distance (KVM switch -- Host)	6 feet (1.8m)
Video Resolution (Local Console)	up to 2048 x 1536@60Hz
Video Resolution (Remote Console)	up to 1600x1200@60Hz
High color depth	16 bits
Remote Control	KVM Console (Java applet, Active X)
	Telnet Console
	Max. 15 users access to the server simultaneously
Serial Port Mode (DB9 male)	Configuration console
	Serial Over LAN (Passthrough access to serial port via Telnet)
	Power control
Protocols	TCP, IP, ARP, ICMP, HTTP/HTTPS, Telnet, DHCP/BOOTP
	SMTP, NTP, DNS, Dynamic DNS
Security	SSL 256-bit Data Encryption
	Secure encryption of keyboard, mouse, and video signals
	Inactivity timeout
Authentication	SSL / Certificate
Event Log Function	Local
	SMTP
	Web pages (HTTP/HTTPS)
	Firmware upgrade via Web interface
	Email notification according to the equipment alarm messages
Virtual Media	CDROM drive redirectiion
	ISO redirectiion
	Floppy/USB drive redirection
	Floppy/USB Image redirection
Housing	Metal
Weight	0.648 Kg
DC Power	5VDC, 2.5A

Operation Temperature	0 ~ 40 ℃ (32 ~ 104 ℉)
Storage Temperature	-20 ~ 50 ℃ (-4 ~ 122 ℉)
Humidity	0~80%, Non-Condensing
Dimension (mm)	158 x 142 x 27

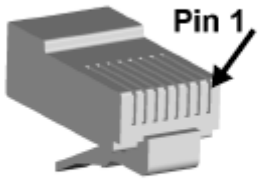
10.2 Default Settings

Server Name	**IP-KVM**
DHCP	**Disable**
IP Address	**192.168.0.1**
Net Mask	**255.255.255.0**
Gateway	**192.168.0.254**
Serial Number	**xxxxxxxxx**(printed on bottom of unit)
MAC Address	**xx:xx:xx:xx**(printed on bottom of unit)
Version & Date	current firmware version number & date
User Name	root
Password	superuser
Protocol (serial)	Telnet
Protocol (web)	HTTP
IP Filter	Disable
Serial ports --	
Baud Rate	9600
Data/Stop	8-1
Parity	None
Flow Control	None

Appendix A: Ethernet pin-outs (RJ-45)

Standard Ethernet Cable RJ-45 Pin-out

Pin	Description
1	Tx+
2	Tx-
3	Rx+
4	NC
5	NC
6	Rx-
7	NC
8	NC



Appendix B: Well-Known TCP/UDP Port Numbers

Port numbers are divided into three ranges: Well Known Ports, Registered Ports, and Dynamic and/or Private Ports. Well Known Ports are those from 0 through 1023. Registered Ports are those from 1024 through 49151. Dynamic and/or Private Ports are those from 49152 through 65535.

Well Known Ports are assigned by IANA, and on most systems, can only be used by system processes or by programs executed by privileged users. Table below shows some of the well-known port numbers. For more details, please visit the IANA website: http://www.iana.org/assignments/port-numbers

Port Number	Protocol	TCP/UDP
21	FTP (File Transfer Protocol)	TCP
22	SSH (Secure Shell)	TCP
23	Telnet	TCP
25	SMTP (Simple Mail Transfer Protocol)	TCP
37	Time	TCP, UCP
39	RLP (Resource Location Protocol)	UDP
49	TACACS, TACACS+	UDP
53	DNS	UDP
67	BOOTP server	UDP
68	BOOTP client	UDP
69	TFTP	UDP
70	Gopher	TCP
79	Finger	TCP
80	HTTP	TCP
110	POP3	TCP
119	NNTP (Network News Transfer Protocol)	TCP
161/162	SNMP	UDP
443	HTTPS	TCP

Appendix C: Protocol Glossary

BOOTP (Bootstrap Protocol)
Similar to DHCP, but for smaller networks. Automatically assigns the IP address for a specific duration of time.

CHAP (Challenge Handshake Authentication Protocol)
A secure protocol for connecting to a system; it is more secure than the PAP.

DHCP (Dynamic Host Configuration Protocol)
Internet protocol for automating the configuration of computers that use TCP/IP.

DNS (Domain Name Servers): A system that allows a network name server to translate text host names into numeric IP addresses.

Kerberos
A network authentication protocol that provides strong authentication for client/server applications by using secret-key cryptography.

LDAP (Lightweight Directory Access Protocol)
A protocol for accessing directory information.

NAT (Network Address Translation)
An Internet standard that enables a LAN to use one set of IP addresses for internal traffic and a second set of addresses for external traffic. This enables a company to shield internal addresses from the public Internet.

NFS (Network File System)
A protocol that allows file sharing across a network. Users can view, store, and update files on a remote computer. You can use NFS to mount all or a portion of a file system. Users can access the portion mounted with the same privileges as the user's access to each file.

NIS (Network Information System)
System developed by Sun Microsystems for distributing system data such as user and host names among computers on a network.

NMS (Network Management System)
NMS acts as a central server, requesting and receiving SNMP-type information from any computer using SNMP.

NTP (Network Time Protocol)
A protocol used to synchronize time on networked computers and equipment.

PAP (Password Authentication Protocol)
A method of user authentication in which the username and password are transmitted over a network and compared to a table of name-password pairs.

PPP (Point-to-Point Protocol)
A protocol for creating and running IP and other network protocols over a serial link.

RADIUS (Remote Authentication Dial-In User Service)
An authentication and accounting protocol. Enables remote access servers to communicate with a central server to authenticate dial-in users and their access permissions. A company stores user profiles in a central database that all remote servers can share.

SNMP (Simple Network Management Protocol)
A protocol that system administrators use to monitor networks and connected devices and to respond to queries from other network hosts.

SMTP (Simple Mail Transfer Protocol)
TCP/IP protocol for sending email between servers.

SSL (Secure Sockets Layer)
A protocol that provides authentication and encryption services between a web server and a web browser.

SSH (Secure Shell)
A secure transport protocol based on public-key cryptography.

TACACS+ (Terminal Access Controller Access Control System)
A method of authentication used in UNIX networks. It allows a remote access server to communicate with an authentication server to determine whether the user has access to the network.

Telnet
A terminal protocol that provides an easy-to-use method of creating terminal connections to a network host.